CLAIMS

1. A group signature system which creates a group signature to prove that the signer is really a member registered in the group and which confirms whether or not said signer of said group signature thus created is really a member of said group, comprising:

a group management device which discloses public information for common use throughout the system, in a referenceable manner from other devices,

a signature device which creates, from a member certificate containing a first element and a second element, encrypted data by encrypting said first element through use of a first random number and said public information disclosed by said group management device; creates first converted data by converting said first element through use of a second random number and said public information; creates second converted data by converting the first element through use of a third random number and the public information; creates knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, said first element, and said second element; and outputs as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message; and

a verification device that verifies whether said group signature has duly been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, based on said message and said group signature outputted from

said signature device and said public information disclosed by said group management device.

2. The group signature system of claim 1, wherein said signature device creates said knowledge signature data in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged; and

said verification device verifies whether said group signature has been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, without using information concerning said first element, said second element, and said signature key.

3. The group signature system of claim 1 or 2, further comprising a member management device which, when registering a new member into said group, selects a member registration private key so that the key will be a generator of a finite field having the order of a prime number; uses a discrete logarithm as said member registration private key; obtains a member registration public key, which is a generator of a multiplicative group on a finite field, from said member registration private key; notifies said member registration public key as public information to said group management device; stores said member registration private key in itself; and creates a member certificate using such member registration private key and notifies the resultant member certificate to said signature device.

4. The group signature system of claim 3, wherein said member certificate is a Nyberg-Rueppel signature which uses said signature key as a discrete logarithm and which is created by using said member registration private key on the converted data from said signature key.

5. The group signature system of claim 3 or 4, wherein said group management device discloses, in addition to said public information, said member information notified by said member management device in a referenceable manner from other devices.

6. The group signature system of claim 1 or 2, further comprising a plurality of member sub-management devices which, when registering a new member into said group, assigns one of the distributed values for obtaining the required generator of a finite field having the order of a prime number as its own distributed member registration private key; stores said distributed member registration private key in itself; and uses as a member registration public key the value having said generator as a discrete logarithm; and wherein

said signature device obtains a member certificate by communicating with a plurality of said member sub-management devices, and

said group management device acquires said member registration public key.

7. The group signature system of any one of claims 1 to 6, further comprising a member tracking device which selects a member tracking private key so that the key will be a generator of a finite field having the order of a prime number; uses a discrete logarithm as said member tracking private key; obtains a member tracking public key that is a generator of a

multiplicative group on a finite field from said member tracking private key; notifies said member tracking public key as said public information to said group management device; stores said member tracking private key in itself; when identifying the signer of a group signature, decrypts the encrypted data contained in said group signature by using said member tracking private key; and, if the result of decryption matches the first element of one of said member certificates which have been disclosed by said group management device, identifies the member of such member certificate as the signer; and wherein

said group management device has disclosed said member certificate as said member information; and

when creating said encrypted data by encrypting said first element, said signature device uses said member tracking public key as said public information.

8. The group signature system of any one of claims 1 to 6, further comprising a plurality of member sub-tracking devices, wherein the distributed member tracking private key for each member sub-tracking device is the one to be assigned to itself, among the distributed values for obtaining the generator of a finite field having the order of a prime number; and each of which obtains said distributed member tracking private key so that the member tracking public key has a discrete logarithm as the generator of said finite field and will be a generator of a multiplicative group on a finite field; and each of which stores said distributed member tracking private key in itself;

when creating said encrypted data by encrypting said first element, said signature device uses said member tracking public key as said public information;

said group management device has disclosed said member certificate as said member information; and

during the process of identifying the signer of a group signature, each of said member sub-tracking devices identifies the member of one of said member certificates as the signer, if the decryption result obtained from the result of performing a pre-determined calculation on the encrypted data contained in said member group signature by using each of their said distributed member tracking private keys matches the first element of one of said member certificates that have been disclosed by said group management device.

9. The group signature system of any one of claims 3, 6, 7 or 8, wherein a finite field on an elliptic curve is used instead of said multiplicative group on a finite field.

10. A group signature method for a group signature system having a group management device, a signature device and a verification device, which creates a group signature to prove that the signer is really a member registered in the group and which confirms whether or not said signer of said group signature thus created is really a member of said group, comprising the steps of:

said group management device

disclosing public information for common use throughout the system, in a referenceable manner from other devices;

said signature device

storing a member certificate consisting of a first element and a second element,

creating encrypted data by encrypting said first element using a first random number and said public information disclosed by said group management device,

creating first converted data by converting said first element using a second random number and said public information,

creating second converted data by converting said first element using a third random number and said public information;

creating knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, said first element, and said second element, in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged, and

outputting as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message, and

said verification device

verifying whether or not said group signature has been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, based on said message and said group signature outputted from said signature device and said public information disclosed by said group management device without using the information concerning said first and second elements and said signature key.

11. A group signature device which forms a group signature system together with a group management device that discloses public information for common use throughout the system in a referenceable manner from other devices and a verification device that confirms whether or not the signer of a group signature is a member registered in said group, and which creates a group signature that can prove that said signer is a member registered in said group, comprising:

a member information storage means which stores a member certificate consisting of a first element and a second element,

an encrypted data creation means which creates encrypted data by encrypting said first element using a first random number and said public information disclosed by said group management device,

a first converted data creation means which creates first converted data by converting said first element using a second random number and said public information,

a second converted data creation means which creates second converted data by converting said first element using a third random number and said public information,

a knowledge signature creation means which creates knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, said first element, and said second element, in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged, and

a signature output means which outputs as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message.

12. A group signature program to be run on a computer to make the computer operate as a group signature device, which forms a group signature system together with a group management device that discloses public information for common use throughout the system in a referenceable manner from other devices and a verification device that confirms whether or not the signer of a group signature is a member registered in said group, in order to create a group signature that can prove that said signer is a member registered in said group, comprising the processes of:

a member information storage means storing a member certificate consisting of a first element and a second element;

an encrypted data creation means creating encrypted data by encrypting said first element using a first random number and said public information disclosed by said group management device;

a first converted data creation means creating first converted data by converting said first element using a second random number and said public information;

a second converted data creation means creating second converted data by converting said first element using a third random number and said public information; and

a knowledge signature creation means creating knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, said first element, and said second element, in such a

manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged; and

a signature output means outputting as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message.